(12)

### **EUROPEAN PATENT APPLICATION**

(43) Date of publication: 13.02.2002 Bulletin 2002/07

(51) Int CI.7: **G07D 7/00**, G06K 19/077, B42D 15/00

(21) Application number: 01119470.1

(22) Date of filing: 13.08.2001

(72) Inventor: Arrieta, Antonio Jesus 6-60311 Frankfurt am Main (DE)

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

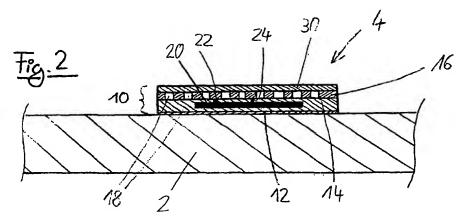
(30) Priority: 11.08.2000 EP 00117474

(71) Applicant: European Central Bank 60311 Frankfurt am Main (DE) (74) Representative:
Luderschmidt, Schüler & Partner GbR
Patentanwälte, John-F.-Kennedy-Strasse 4
65189 Wiesbaden (DE)

### (54) Security document and process for producing a security document

(57) The present invention relates to a security document 2 comprising a hologram 10 and an emitter device 20, 26 for emitting predetermined data in a noncontacting manner. The emitter device comprises an integrated circuit 20 and an antenna 26 connected to the integrated circuit. According to the invention, the emitter device is integrated into the hologram. In a preferred

embodiment of the invention the integrated circuit is integrated into the substrate 14 of the hologram and the metal layer of the hologram forms the antenna which is connected to the integrated circuit. This combination means important improvement, from the point of view of product usage, and the occurrence of a hiding effect, a protection effect and the emission usage of the hologram for the radio frequency emitter device.



EP 1 179 811 A1

#### Description

20

30

45

[0001] This invention relates to a security document and a process for producing a security document.

**[0002]** The identification and authentication of security documents, such as banknotes, checks, stocks, bonds, passports, identity cards etc, is a long-standing problem. One of the proposes of the different security devices included in the above mentioned security documents is to store information that allows both users and machines to discriminate between real and forged documents and to discriminate among different real security documents.

[0003] There have been adopted different techniques in order to achieve an easy and secure authentication and/or identification of security documents, especially banknotes. These techniques make use of special papers, special inks and special patterns, the inclusion of watermarks and the inclusion of plastics, metal or magnetic strips.

[0004] Above all, it is known to embed a flat chip in a bank note. The first surface of the chip is attached to a metal carrier plate to increase the mechanical stability of the chip and to simplify the handling of the chip during the production of the security document. On the second surface of the chip there is provided a layer serving as a protection against chemical attacks due to an aggressive environment. The chip stores data which might be read out by another device in a noncontacting manner. A bank note including a chip is described in the German Patent DE 196 01 358.

[0005] The transponder of the known banknote is preferably arranged in the vicinity of the metal strip of the banknote in order to increase the mechanical stability of the transponder. The antenna is formed by the metal strip of the banknote. To provide a protection against chemical attacks, the transponder is embedded in a sealing compound.

[0006] A banknote and, in general, a security document is used by the public. As the general public should not notice the incorporation of a security device, it is necessary to hide it in order to prevent destructive manipulation and illegal modification attempts.

[0007] In all commercial radio frequency emitter devices, the most evident part is the antenna (in loop size, straight, etc.). The perception of these elements makes the user aware of the presence of a radio frequency emitter device. Security documents as banknotes, passports, checks, etc. are handled under quite different conditions. Those documents must be strong enough for resisting environmental, chemical and mechanical attacks. This is part of the normal life of those security documents. These normal life conditions of a banknote or security document can be quite dangerous for a sophisticated electronic device, like the security device, if is not sufficiently protected.

[0008] Both the energising and communication between an external reader/writer device and the security device inserted in the security document is accomplished through an antenna. For that reason the electronic device inserted in the security document must be equipped with a proper antenna to guarantee a good electromagnetic signal transmission and reception.

[0009] Antennas can be made using conductor elements in different shapes and lengths resonating at the wavelength used. Longitudinal antennas are usually not used for the big length necessary in order to maximise the effect. In fact, for a typical 13.56 MHz frequency transmission, the length of the antenna should be 22.12 meters; this is not practical at all for security documents due to the size of the document needed and how evident that it becomes be for the public.

**[0010]** A banknote production process is a quite complex and expensive combination of paper making, printing and holograms stamping. The inclusion of a new element, like a radio frequency emitter device, in a security document adds a new step to the manufacturing process with the subsequent cost increase due to the machine using, manpower, raw materials, waste, etc.

[0011] A banknote comprising a security device is described in the published German Patent Application DE 196 30 648 A1. The security device utilises an antenna to exchange the information with an external reader/writer device via the transmission of an electromagnetic signal through the generation of an induced voltage in the antenna. With the use of an energising radio frequency signal, the reader/writer device can communicate with the security device inserted in the banknote without the necessity of any external power source such as a battery. Such devices are well known as transponders.

[0012] It is an object of the invention to provide a security document comprising an improved security device preventing destructive manipulation and illegal modification attempts and being strong enough for resisting environmental, chemical and mechanical attacks. Another object of the invention is to provide a cost saving process for producing a security document comprising a security device.

50 [0013] These objects are solved by a security document and a process for producing the security document comprising the features of claims 1, 7 and 8, respectively. Further advantageous aspects of this invention are subject matter of the dependent claims.

[0014] According to the invention, the following advantages arise as a consequence of the combination of an radio frequency emitter device and a hologram in its combined usage both for security documents protection and identification.

[0015] This combination of an emitter device for emitting predetermined data in a noncontacting manner with a hologram will preferably consist in the embedding of the emitter device in the hologram substrate and the connection of the emitter device to the metal layer of the hologram.

[0016] These advantages can be split in product performance and in process performance. From the point of view of the product performance, three advantages are obtained as a consequence of this combination: a hiding effect, a protection effect and an antenna effect of the hologram for the radio frequency emitter device.

[0017] From the point of view of the process performance, the main advantage is cost saving in the document production process.

[0018] As mentioned before, this combination means important improvement, from the point of view of product usage, and the occurrence of a hiding effect, a protection effect and the emission usage of the hologram for the radio frequency emitter device. These product improvements are explained as follows.

[0019] Holograms are widely used in security documents as an authentication feature due to the impossibility of reproduction by illegal way. Users of security documents are aware of these elements and recognise them as a proof of authenticity.

[0020] The inventor has recognized that holograms have large-enough surfaces in order to integrate the antenna for the radio frequency emitter device and to hide the radio frequency emitter device.

[0021] With this hiding effect, the security of the radio frequency emitter device is improved due to the impossible access for the public and, therefore, the impossible illegal manipulation of the device. Also, any attempt of physical manipulation by the public of the radio frequency emitter device will mean the destruction of the hologram and the loss of authenticity of the security document.

**[0022]** According to the prior art, the transponders are protected by separate layers or sealing compounds. In contrast to the known security documents, the partial destruction of the hologram is easily recognizable since the hologram is subject of a visual inspection or examination.

[0023] The inclusion of the emitter device in the hologram confers on it a unique protective layer from environmental, mechanical and chemical attacks.

[0024] The use of a radio frequency emitter device combined with a hologram means an important process cost saving in comparison with the application of a device of these characteristics, in a separately process, on a security document.

[0025] The integration of a radio frequency emitter device with a hologram means cost saving in machine using, because this new combined security element can be applied at the same production step that a normal hologram. The cost reduction comes from the saving in machinery, manpower, waste, etc. It is also expected that the raw material cost of this combined new element would be lower than the cost of a hologram and a radio frequency emitter device separately.

[0026] Crucial requests for any security document production facility are security of the installations, control on produced goods and security elements used. The applying of holograms to security documents requires strict control of the amount of holograms used, both applied and wasted ones. The combination of the emitter device and the hologram allows the security documents producer to control in a faster and more secure way any single element of this combination, and a quite easy deactivation of the radio frequency emitter device in the waste.

[0027] As mentioned before, a major aspect of the invention is that the metal layer of the hologram is at least partially formed like an antenna, the emitter device being connected to the antenna-like metal layer, i. e. the metal layer of the hologram forms the antenna of the radio frequency emitter device.

[0028] Using an antenna integrated in a hologram, once the security document with emitter device integrated in a hologram is in close proximity to the external reader/writer device, the time-varying electromagnetic field B that is produced by this external device induces a voltage (called electromotive force or simply EMF) in the antenna integrated in the hologram. The induced voltage in the antenna integrated in the hologram causes a flow of current on this metal layer. The law that explains this phenomenon is called Faraday's law: the induced voltage on the antenna integrated in the hologram is equal to the time rate of change of the electromagnetic flux  $\mathbf{g}$ . The voltage generated in the antenna integrated in the hologram will depend on the current that circulates on the external reader/writer device, the extension of the hologram integrated antenna of the security device and the distance between both devices.

[0029] The current flow in the external reader/writer device produces a magnetic flux that causes a voltage induction at the antenna integrated in an hologram inserted in the security element. The voltage induced in the antenna portion of the metal layer may be calculated by the following equation:

$$V = -N_2 \frac{d\Psi}{dt} = -N_2 \frac{d}{dt} \left( \int B \cdot dS \right) = -N_2 \frac{d}{dt} \left[ \int \frac{\mu_0 i_1 N_1 a^2}{2(a^2 + r^2)^{3/2}} \cdot dS \right] = -\left[ \frac{\mu_0 N_1 N_2 a^2 (\pi b^2)}{2(a^2 + r^2)^{3/2}} \right] \frac{di_1}{dt} = -M \frac{di_1}{dt}$$

where:

15

20

25

35

45

50

55

V = voltage induced in the antenna integrated in the hologram

Ψ= Magnetic flux through each turn

B = magnetic field

5

10

15

20

25

30

40

45

50

N<sub>2</sub>= number of loops in the integrated antenna

 $i_1$  = current on the external reader/writer antenna

a = radius of the external reader/writer antenna

b = radius of the integrated antenna

 $N_1$  = number of loops in the antenna of the reader/writer device.

r = distance between the two antennas.

M = mutual inductance between the two antennas.

$$M = \left[ \frac{\mu_0 N_1 N_2 (ab)^2}{2(a^2 + r^2)^{3/2}} \right]$$

[0030] As shown in the above equation, the voltage in the antenna integrated in a hologram is largely dependent on the mutual inductance between the two antennas. This mutual inductance is a function of the antenna geometry and the distance between them. As can be deduced the above equation, induced voltage in the antenna integrated in a hologram decreases with the distance between this element and the external reader/writer device at the cubic potency. For that reason the usage of an hologram for integrating the antenna, that is always in the security element surface means an important improvement for signal transmission, due to the important reduction of the distance with the external reader/writer device.

[0031] Antenna size is the second parameter that maximises the induced magnetic field. For different shapes of antennas - like a circular one loop antenna, a circular several loop antenna and a square loop antenna - as a rectangular cross section, the inductance is maximised when the thickness is reduced.

[0032] Using as antenna the metallic layer of an hologram maximises the inductance of all of those sort of antennas, because of the extremely thin hologram metal layer used for this proposal. Therefore, the electrical current produced in the antenna integrated in the hologram is maximised when the security document comes into the field created by the external reader/writer device.

[0033] Also, using as antenna the metallic layer of a hologram due to the precision of the hologram manufacturing process, all shapes of antenna can be easily produced and for each specific transmission requirement different antenna integrated in hologram shapes can be produced.

[0034] The magnetic flux through the antenna is maximised when the antenna loop is perpendicular to the electromagnetic field. This is due to the inner product of two vectors, as is the case of the electromagnetic field and the surface of the hologram integrated antenna, which is maximised when they are perpendicular, so the cosine of the angle reaches its maximum value, 1. The hologram applied to a security document remains always in the same position on the surface. The integration of an antenna in an hologram makes the antenna remaining always parallel to the security document surface and perpendicular to any external reader/writer device. Therefore, the voltage in the hologram integrated antenna is maximised.

[0035] According to a preferred embodiment of the invention, the metal layer is partially formed like a loop size antenna. Loop size antennas are more feasible than longitudinal ones, and as Faraday's law states that a time-varying electromagnetic field through a surface bounded by a closed path induces a voltage around the loop, the transmission and reception effect is also reached.

[0036] Loop size antennas can be easily manufactured using the metal layer of the hologram, and the final result of this combination reaches the technical necessities electromagnetic signals transmission/reception and the necessary discretion for the emitter device once inserted in the security document.

[0037] Holograms that are used in security documents consist in few microns of metal (usually aluminium) over a plastic substrate. The advanced technology used in this manufacturing process makes different sizes of loops, as circular, rectangular, etc. easy available.

[0038] The antenna portion of the metal layer may be circular with a single loop. The inductance for a single loop circular antenna portion integrated in the metal layer is:

55

$$L = 0.01257a \left[ 2.303 \log_{10} \left( \frac{16a}{d} - 2 \right) \right] (\mu H)$$

where:

10

15

25

30

35

a= mean radius of the hologram integrated antenna loop, in cm l= length of the integrated antenna, in cm

[0039] According to a further aspect of the invention the metal layer is at least partially formed like a loop size antenna having multiple loops. The antenna portion of the metal layer may for example be circular with multiple loops. The inductance for a multiple loop circular antenna inductor is:

 $L = \frac{0.31(aN)^2}{6a + 9b + 10h} (\mu H)$ 

20 where:

a = mean radius of the hologram integrated antenna loop, in cm

N = number of loops of the integrated antenna

h = thickness of the film of the integrated antenna

b = winding length of the integrated antenna, in cm

[0040] According to a further aspect of the invention the security device is attached to the security document via an adhesive layer disposed on the surface of the substrate of the hologram opposite to the surface with the metal layer thereon.

[0041] According to another aspect of the invention the security document is a banknote.

[0042] The invention can be more clearly understood by means of preferred embodiments of the invention which are described in the following in conjunction with the accompanying drawings, where

- Fig. 1 shows a diagrammatic, perspective view of a security document according to the invention with a security device according to the invention,
- Fig. 2 shows an expanded vertical cross-section view taken through the security document of figure 1 at the location of the security device according to the invention,
- Fig. 3 shows a top view of the security device of figure 1 and 2 according to a first embodiment of the invention and
- Fig. 4 shows a top view of the security device of figure 1 and 2 according to a second embodiment of the invention.

[0043] Figure 1 shows a perspective view of a security document 2 according to the invention, such as banknotes, checks, stocks, bonds, passports, identity cards etc. The security document comprises a hologram 10. On the security document 2 there is further provided a radio frequency emitter device 4. Along with the emitter device 4 there may also provided other security elements, for example a metal strip 6 being partially embedded in the security document 2 or a watermark 8.

[0044] Figure 2 shows an expanded vertical cross-section view taken through the security document of figure 1 at the location of the emitter device 4. The emitter device 4 is part of the hologram 10 of the security document.

[0045] The hologram 10 comprises a substrate 14 which is usually used in holograms and which may be made of plastic and a metal layer 16 provided on the substrate. The metal layer 16 is usually made of aluminium. The substrate is attached to the security document via an adhesive layer 12.

[0046] On the metal layer 16, which comprises recesses 18 forming the hologram, there is provided a transparent layer 30 for protection of the metal layer 16 from environmental, chemical or mechanical attacks.

[0047] According to the invention, the emitter device 4 comprises an integrated circuit 20 which could be a transponder. The integrated circuit 20 comprises a storing device for storing data for the identification and authentication of the banknote. The data can be read out in a noncontacting manner, as will be described later.

[0048] In the embodiment shown in figure 2, the integrated circuit 20 is integrated into the substrate 14 of the hologram element 10, i. e. the transponder 20 is completely surrounded by the material of the substrate 14 so that an excellent protection of the transponder 20 against environmental influences is achieved. The integrated circuit 20 further com-

prises two connections 22, 24 each extending between the circuit 20 and the metal layer 16 so that the circuit is connected with the metal layer 16 or at least a part of it.

[0049] Figure 3 shows a top view of the emitter device 4 of figures 1 and 2 according to a first embodiment of the invention. The metal layer 16 comprises an antenna portion 26, which is shown with a hatching. The antenna portion 26 is connected with the integrated circuit 20 (fig. 2) via the connections 22, 24 and is essentially ring-shaped. In order to achieve an unhindered flow of current from one connection 22, 24 through the antenna portion 26 to the other connection 24, 22, it is preferred that the antenna portion 26 is completely separated from the other portions of the metal layer 26 by a recess 28. It should be noted that the other portions of the metal layer 16 are merely shown schematically.

[0050] Figure 4 shows a top view of the emitter device 4 of figures 1 and 2 according to a second embodiment of the invention. The main difference between the first embodiment shown in figure 3 and the second embodiment of figure 4 is that the antenna portion 26' in figure 4 is spiral-shaped so that the antenna portion comprises multiple loops. It should be noted that the antenna could be designed in any shape.

[0051] The security document 2 comprising the emitter device 4 will be brought in close proximity to an external reader/writer device (not shown). The external reader/writer device produces a time-varying electromagnetic field *B*. Thus, a voltage (called electromotive force or simply EMF) is induced in the antenna portion 26, 26' of the metal layer 16 of the hologram element 10. The induced voltage in the antenna portion 26, 26' of the hologram element 10 causes a flow of current in the antenna portion 26, 26'. Since the integrated circuit 20 (transponder) is connected with the antenna portion 26, 26' via connections 22, 24, the transponder 20 is supplied with electric power. As a result, the transponder 20 sends a signal being representative for the information being stored in the storing device. This signal is received by the external reader/writer device. Thus, the information inside the storing device of the transponder 20 has been made available.

#### Claims

25

30

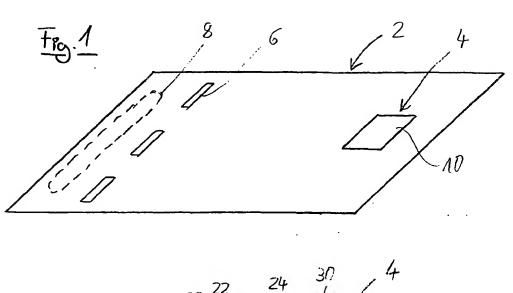
40

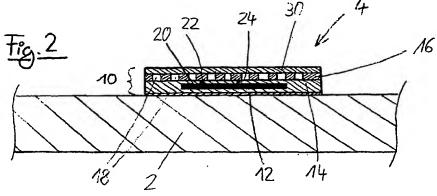
45

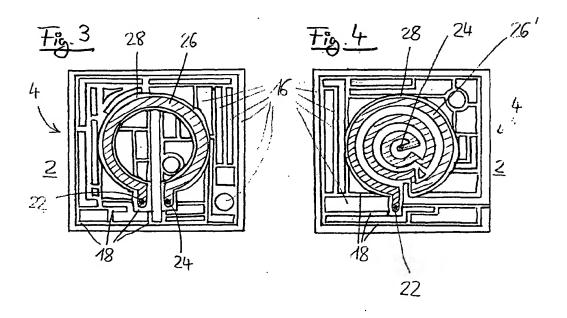
50

- 1. Security document comprising a hologram (10) and an emitter device (20, 26) for emitting predetermined data in a noncontacting manner, the emitter device comprising an integrated circuit (20) and an antenna (26) connected to the integrated circuit, characterized in that the emitter device (20, 26) is integrated into the hologram (10).
- Security document according to claim 1, wherein the hologram (10) comprises a substrate (14) with a metal layer (16) disposed on at least one surface thereof, the integrated circuit (20) being integrated into the substrate of the hologram.
- 35 3. Security document according to claim 2, wherein the substrate (14) is attached to the security document via an adhesive layer (12) disposed on the side of the substrate opposite to the side with the metal layer (16) thereon.
  - 4. Security document according to one of claims 2 and 3, wherein the metal layer (16) is at least partially formed like an antenna, the integrated circuit (20) being connected to the antenna-like metal layer (26).
  - 5. Security document according to claim 4, wherein the metal layer (16) is partially formed like a loop size antenna (26).
  - Security document according to claim 4, wherein the metal layer (16) is partially formed like a loop size antenna having multiple loops (26').
    - 7. Security document according to one of claims 1 to 5, wherein the security document (2) is a banknote.
    - 8. Process for producing a security document of one of claims 1 to 7 comprising the step of integrating the emitter device into the hologram.
    - 9. Process according to claim 8, wherein the integrated circuit of the emitter device is integrated into the substrate of the hologram.
- 10. Process according to one of claims 8 and 9, wherein the metal layer of the hologram is at least partially formed like an antenna and the integrated circuit is connected to the antenna-like metal layer.

ı









## **EUROPEAN SEARCH REPORT**

Application Number EP 01 11 9470

	DOCUMENTS CONSID	ERED TO BE RELEVANT	···	
Category	Citation of document with in of relevant pass	ndication, where appropriate, ages	Retevant to claim	CLASSIFICATION OF THE APPLICATION (Int.CI.7)
X Y A	FR 2 802 001 A (GEM 8 June 2001 (2001-0 * page 3, line 4 - * page 3, line 11 - * page 3, line 17 - * page 4, line 1 - * page 7, line 33 - figures 2,3 *	6-08) line 6 * line 14 * line 25 * line 8 *	1-3,8,9 7 4,10	G07D7/00 G06K19/077 B42D15/00
Y A		D ELEKTRONISCHE ober 1998 (1998-10-29) - line 61; figures *	7 1,4-6	
A	DE 197 34 855 A (WH PRÜFTECHNIK) 18 Feb * claims 1,6,9,10,1	ruary 1999 (1999-02-18)	1,4-7	
A	DE 196 30 648 A (DI 5 February 1998 (19 * page 2, line 2 -		1,4,7,8,	TECHNICAL FIELDS SEARCHED (Int.CI.7) G07D G06K B42D
	The present search report has	been drawn up for all claims		
	Place of search	Date of completion of the search		Examiner
	THE HAGUE	19 November 2001	Nev	ille, D
X: par Y: par doc A: ted O: nor	ATEGORY OF CITED DOCUMENTS ilcularly relevant if taken alone licularly relevant if combined with anot unent of the same category notogical background 	L ; document cited t	curnent but publi te in the application or other reasons	ished on, or

# ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 01 11 9470

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-11-2001

Patent documer cited in search rep		Publication date		Patent fam member(:		Publicatio date
FR 2802001	Α	08-06-2001	FR	2802001	A1	08-06-200
			AU	2522701		18-06-200
			WO	0143066	A1	14-06-200
DE 19718916	Α	29-10-1998	DE	19718916	A1	29-10-1998
			ΑU	8208298	Α	24-11-199
			AU	8208498		24-11-1998
			BG	103838		30-06-2000
			BG	20000	A	28-04-200
			BR	9809776		05-09-200
			BR	9809777	A	05-09-200
			CN	1253648	T	17-05-200
			CN	1253649		17-05-2000 05-11-1990
			WO WO	9849657 9849655		05-11-1998
			DE	19812812		23-09-199
			EP	0978107		09-02-200
			ĒΡ	0978108		09-02-200
			ĤŬ	0002699		28-12-200
			HU	0003820		28-02-200
			LV	12423		20-01-200
			LV	12423	В	20-05-200
			LV	12424	Α	20-01-200
			LV	12424	В	20-05-200
			NO	994725	Α	23-12-199
			NO	994726	Α	22-12-199
			PL	336525		03-07-200
			PL	336534		03-07-200
			TR	9902662		21-02-200
			TR	9902663	12 	21-02-200
DE 19734855	Α	18-02-1999	DE	19734855		18-02-199
			AU	8208198		08-03-199
			AU BG	8208398 104142		08-03-199 30-06-200
			BG BG	104142		30-06-200
			BR	9811149		25-07-200
			BR	9811153		25-07-200
			CN	1267383	Ť	20-09-200
			CN	1265761	Ť	· 06-09-200
			WO	9909527	A1	25-02-199
			WO	9909528		25-02-199
			DE	19812811		23-09-199
			EP	1004097	A1	31-05-200
			EP	1002300	A1	24-05-200
		e Official Journal of the	HU	0003358	A2	28-02-200
		<u> </u>				

# ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 01 11 9470

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-11-2001

Patent document cited in search rep		Publication date		Patent fam member(s		Publication date
DE 19734855	A		HU JP NO NO PL PL SK	0003759 2001516092 20000615 20000616 338473 340874 1782000	T A A A1 A1 A3	28-02-2001 25-09-2001 07-04-2000 07-04-2000 06-11-2000 12-03-2001 09-10-2000
			SK TR	1932000 200000651	T2	11-12-2000 21-08-2000
DE 19630648	A	05-02-1998	DE	19630648	A1	05-02-1998
				•		
				•		

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82